# 【「iOS」「Android」とのVPN（IKEv2/IPsec）接続-IPv4（Si-R GX500）】

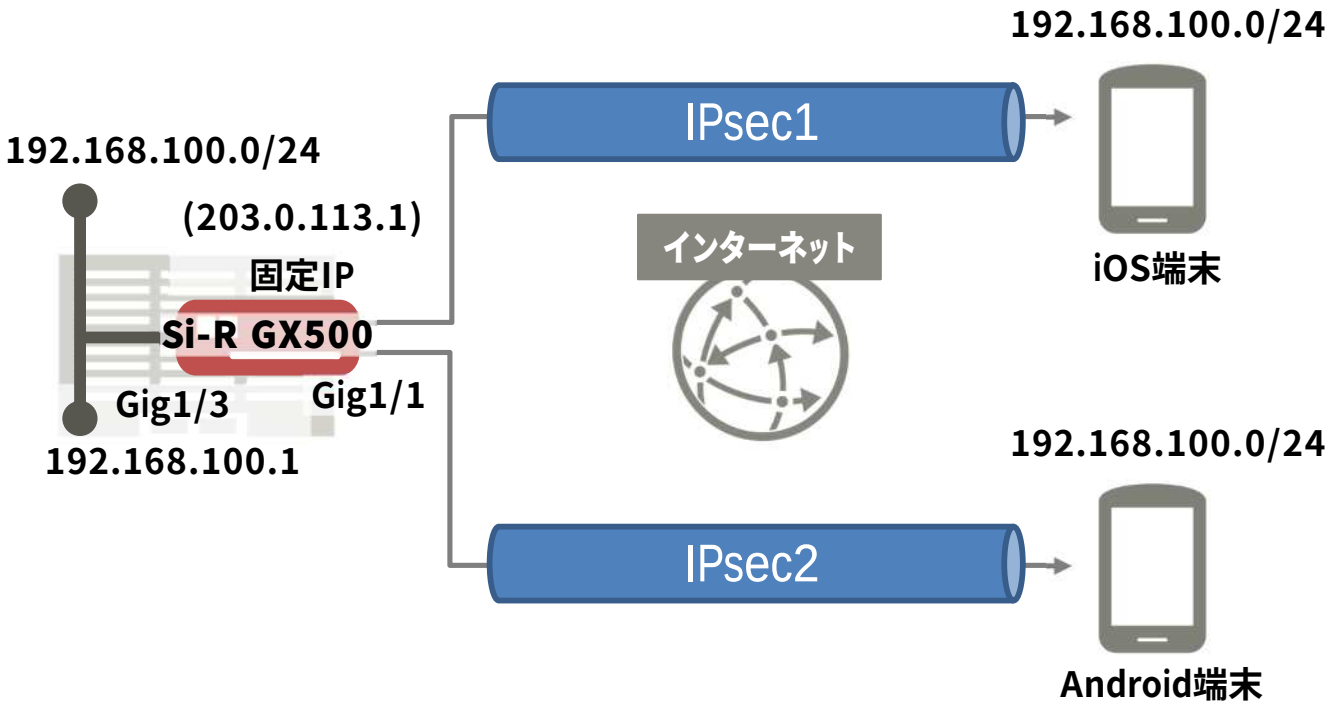
「iOS端末」「Android端末」とIPv4でリモートアクセスVPN（IKEv2/IPsec）接続する設定例です。
※本設定例は、弊社で独自に接続試験を行った結果を元に作成しております。

## [対象機種と版数]

Si-R GX500 V01.14以降
iOS 16.5.1
Android V12

## [設定内容]

- Si-RGX500のWAN側をGigabitethernet1/1、LAN側をGigabitethernet1/3とします。
- Si-R GX500のWANにはプロバイダより203.0.113.1の固定IPアドレスが割りてられるものとします。
- Si-R GX500のLAN側に192.168.100.1/24を割り当てます。
- iOS端末、Android端末に192.168.100.0/24（192.168.100.200～192.168.100.250）を割り当てます。



# [設定]

以下の設定例を、コピー&ペーストでご利用いただくことができます。

- test1 にはiOSのローカルIDを設定してください。
- sir-key1 にはiOSのシークレット（IPsec 共有鍵）を設定してください。
- test2 にはAndroidのIPsec IDを設定してください。
- sir-key2 にはAndroidのIPsec事前共有鍵を設定してください。
- id-a@ispにはSi-RのISPのIDを設定してください。
- pwd-a@ispにはSi-RのISPのパスワードを設定してください。

## ■ Si-R GX500設定

```
access-list 111 permit udp any host 203.0.113.1 eq 500
access-list 111 permit udp any host 203.0.113.1 eq 4500
access-list 111 permit icmp any host 203.0.113.1
access-list 111 permit 50 any host 203.0.113.1
!
ip route 0.0.0.0 0.0.0.0 tunnel 1
ip local pool POOL1 192.168.100.200 192.168.100.250
!
logging buffer level informational
!
aaa authorization network CP1 local-group CONFIG1
!
crypto ipsec udp-encapsulation nat-t keepalive interval 60
!
crypto ipsec policy P2
 set pfs group2 group5 group14 group15
 set security-association lifetime seconds 3600
 set security-association transform-keysize aes 128 256 256
 set security-association transform esp-aes esp-sha-hmac esp-sha256-hmac
 set mtu 1454
 set mss auto
 set ip tos copy
 set ip df-bit 0
 set ip fragment post
 sa-up route
exit
!
crypto ipsec selector SELECTOR
 src 1 ipv4 any
 src 2 ipv6 any
 dst 1 ipv4 any
 dst 2 ipv6 any
exit
!
```

```
crypto isakmp keepalive interval 30
crypto isakmp log sa
crypto isakmp log session
crypto isakmp log negotiation-fail
!
crypto isakmp client configuration group CONFIG1
 pool POOL1
exit
!
crypto isakmp policy P1
 authentication pre-share
 encryption aes
 encryption-keysize aes 128 256 256
 group 2 5 14 15
 lifetime 86400
 hash sha sha-256 sha-384 sha-512
exit
!
crypto isakmp profile remote
 local-address 203.0.113.1
 set isakmp-policy P1
 set ipsec-policy P2
 keyring KEY1
 ike-version 2
 client configuration address respond
 isakmp authorization list CP1
exit
!
crypto session identification address
!
crypto keyring KEY1
 pre-shared-key host test1 key sir-key1
 pre-shared-key host test2 key sir-key2
exit
!
crypto map MAP1 ipsec-isakmp dynamic
 match address SELECTOR
 set isakmp-profile remote
exit
!
interface GigaEthernet 1/1
 channel-group 1
 speed-duplex auto
 media auto
 pppoe enable
exit
!
interface GigaEthernet 1/3
 channel-group 3
 speed-duplex auto
 media auto
exit
!
```

```
interface Port-channel 1
 mtu 1454
 mss 1414
exit
!
interface Port-channel 3
 ip address 192.168.100.1 255.255.255.0
exit
!
interface Tunnel 1
 ip access-group 111 in
 tunnel mode pppoe profile pppoe-profile
 pppoe interface gigaethernet 1/1
exit
!
pppoe profile pppoe-profile
 authentication accept chap
 account id-a@isp pwd-a@isp
exit
!
end
```

## ■ iOS端末の設定

・ホーム画面から「設定」を選択します。
・設定画面から「一般」を選択します。
・一般画面から「VPNとデバイス管理」を選択します。
・VPNとデバイス管理から「VPN」を選択します。
・VPN画面から「VPN構成を追加...」を選択します。
・VPN構成画面で、以下のように設定します。


・タイプ　　：IKEv2
・説明　　：GX500（任意の文字列）
・サーバ　　：203.0.113.1
　（Si-R GX500のWAN側IPアドレス）
・リモートID　　：203.0.113.1
　(Si-R GX500のWAN側IPアドレス)
・ローカルID　　：test1
・ユーザ認証　　：なし
・証明書を使用　　：オフ
・シークレット　　：sir-key1
・プロキシ　　：オフ

・VPN構成「GX500」が作成されますので、状況をタップしてください。
・IKEv2/IPsecが正しく接続されると状況が「接続済み」となります。

## ■ Android端末の設定

・メニュー画面から「設定」を選択します。
・設定画面から「ネットワークとインターネット」を選択します。
・ネットワークとインターネット画面から「VPN」を選択します。
・VPNとデバイス管理から「+」を選択します。
・VPN構成画面で、以下のように設定します。


・名前　　：GX500（任意の文字列）
・タイプ　　：IKEv2/IPsec PSK
・サーバアドレス　　：203.0.113.1
（Si-R GX500のWAN側IPアドレス）
・IPsec ID　　：test2
・IPsec事前共有鍵　：sir-key2

・VPN「GX500」が作成されますので、GX500に接続の「接続」をタップしてください。
・IKEv2/IPsecが正しく接続されると「接続されました」となります。

# [解説]

## ■ Si-R GX500設定解説

**access-list 111 permit udp any host 203.0.113.1 eq 500**
**access-list 111 permit udp any host 203.0.113.1 eq 4500**
**access-list 111 permit icmp any host 203.0.113.1**
**access-list 111 permit 50 any host 203.0.113.1**
アクセスリストを設定します。
IKEv2/IPsecとICMPのみ透過します。

**ip route 0.0.0.0 0.0.0.0 tunnel 1**
デフォルトルートをWAN側（PPPoEトンネルインタフェース）に向けて設定します。

**ip local pool POOL1 192.168.100.200 192.168.100.250**
IPsecにより通知するIPアドレス範囲を設定します。

**logging buffer level informational**
ログレベルを設定します。

**aaa authorization network CP1 local-group CONFIG1**
IPsecの許可方式として装置内に設定したデータベースを設定します。

**crypto ipsec udp-encapsulation nat-t keepalive interval 60**
NATトラバーサルを行います。

**crypto ipsec policy P2**
**set pfs group2 group5 group14 group15**
**set security-association lifetime seconds 3600**
**set security-association transform-keysize aes 128 256 256**
**set security-association transform esp-aes esp-sha-hmac esp-sha256-hmac**
**set mtu 1454**
**set mss auto**
**set ip tos copy**
**set ip df-bit 0**
**set ip fragment post**
**sa-up route**
**exit**
IPsecポリシーのエントリを設定します。
-Diffie-Hellmanの設定：グループ2,5,14,15
-IPsec-SAの生存時間：3600秒
-AES鍵長：128,256
-暗号アルゴリズム：AES
-認証アルゴリズム：esp-sha-hmac,esp-sha256-hmac
-MTU長：1454byte
-MSS書換：auto
-TOS：元パケットをコピー
-DFビット：0
-フラグメント：ポストフラグメント
-SAのセレクタの宛先情報を経路として登録：登録する

```
crypto ipsec selector SELECTOR
 src 1 ipv4 any
 src 2 ipv6 any
 dst 1 ipv4 any
 dst 2 ipv6 any
exit
```
IPsecSA用セレクタのエントリの設定をします。
送信元/送信先にIPv4/IPv6すべてのアドレスを指定します。

```
crypto isakmp keepalive interval 30
crypto isakmp log sa
crypto isakmp log session
crypto isakmp log negotiation-fail
```
IPsec情報をログに出力します。

```
crypto isakmp client configuration group CONFIG1
 pool POOL1
exit
```
Mode-config/Config Payloadを利用して通知するアドレスプール名を設定します。

```
crypto isakmp policy P1
 authentication pre-share
 encryption aes
 encryption-keysize aes 128 256 256
 group 2 5 14 15
 lifetime 86400
 hash sha sha-256 sha-384 sha-512
exit
```
IKEポリシーのエントリを設定します。
- -認証方式：Pre-shared key
- -暗号アルゴリズム：AES
- -AES鍵長：128,256
- -Diffie-Hellmanの設定：グループ2,5,14,15
- -IKE-SAの生存時間：86400秒
- -ハッシュアルゴリズム：sha-256,sha-384,sha-512

```
crypto isakmp profile remote
 local-address 203.0.113.1
 set isakmp-policy P1
 set ipsec-policy P2
 keyring KEY1
 ike-version 2
 client configuration address respond
 isakmp authorization list CP1
exit
```
IPsecのプロファイルを設定します。
- -ローカルIPアドレス：203.0.113.1
- -IKEポリシー：P1
- -IPsecポリシー：P2
- -IKEバージョン：v2
- -keyring名：KEY1
- -Mode-config/Config Payloadのアドレス払い出し動作（server側）：Request/Reply方式
- -許可方式名：CP1

**crypto session identification address**
セッションの識別をピア／本装置のアドレス、ポートで識別します。

**crypto keyring KEY1**
**pre-shared-key host test1 key sir-key1**
**pre-shared-key host test2 key sir-key2**
**exit**
VPNピアごとにPre-shared Keyを設定します。

**crypto map MAP1 ipsec-isakmp dynamic**
**match address SELECTOR**
**set isakmp-profile remote**
**exit**
VPNセレクタを設定します。
-IPsecセレクタ名：SELECTOR
-IPsecプロファイル名：remote

**interface GigaEthernet 1/1**
**channel-group 1**
**speed-duplex auto**
**media auto**
**pppoe enable**
**exit**
WAN側インタフェースを設定します。
-チャネルグループ：1
-Speed/Duplex：auto
-メディアタイプ：auto
-PPPoE：利用

**interface GigaEthernet 1/3**
**channel-group 3**
**speed-duplex auto**
**media auto**
**exit**
LAN側インタフェースを設定します。
-チャネルグループ：3
-Speed/Duplex：auto
-メディアタイプ：auto

**interface Port-channel 1**
**mtu 1454**
**mss 1414**
**exit**
WAN側のポートチャネルの設定をします。
-MTU：1454byte
-MSS：1414byte

**interface Port-channel 3**
**ip address 192.168.100.1 255.255.255.0**
**exit**
LAN側のポートチャネルの設定をします。
-IPアドレス：192.168.100.1

```
interface Tunnel 1
 ip access-group 111 in
 tunnel mode pppoe profile pppoe-profile
 pppoe interface gigaethernet 1/1
exit
```
PPPoEインタフェースの設定を行います。
  -アクセスリスト（受信側）：ACL111を透過（それ以外は遮断されます）
  -PPPoEプロファイル名：pppoe-profile
  -PPPoEインタフェース：gigaethernet 1/1

```
pppoe profile pppoe-profile
 authentication accept chap
 account id-a@isp pwd-a@isp
exit
```
PPPoEのプロファイルを設定します。
  -認証方式：CHAP
  -ID：id-a@isp
  -Password：pwd-a@isp